Ackton Pastures Primary Academy
Online Safety Policy

Date	Review Date	Coordinator	Nominated Governor
September 2019	September 2020	SLT	Chair

Schedule for Development / Monitoring / Review:

This Online Safety policy was approved by the Governing board on:
22nd July 2019

The implementation of this Online Safety policy will be monitored by the:
Online Safety Lead

Monitoring will take place at regular intervals:
Termly

The Local Governing Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: July 2020.

Should serious online safety incidents take place, the following external persons / agencies should be informed:

The academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Policy

This policy applies to all members of the academy community *(including staff, pupils, volunteers, parents / carers, visitors, community users)* who have access to and are users of academy / academy digital technology systems, both in and out of the *academy*.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data in serious circumstances (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the academy Behaviour Policy. The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of academy.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *academy*:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Board* has taken on the role of *Online Safety Governor.*
The role of the Online Safety Governor is as follows:

- meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings (where possible)
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governing Board

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in academy who carry out the internal online safety-monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / MAT
- liaises with academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets and communicates regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

Network Manager / Technical staff - Alamo

The Network Manager / Technical Staff are responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can

be reported to the Headteacher and the Online Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

Are responsible for ensuring that:
- they have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher, Online Safety Lead for investigation / action / sanction.
- all digital communications with pupils, parents and carers should be on a professional level and only carried out using official academy systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, ipads, cameras etc in lessons and other academy activities and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Team

The Online Safety Team provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety

and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Board.*

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production / review / monitoring of the academy Online Safety Policy / documents.
- Feeding back to computing curriculum lead over opportunities and coverage
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified

Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of academy and realise that the *academy's* Online Safety Policy covers their actions out of academy, if related to their membership of the academy

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns. Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events
- access to parents' sections of the website and on-line student / pupil records

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of *pupils* in online safety / digital literacy is therefore an essential part of the online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited:

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Additional duties for the academy / academies under the Counter Terrorism and Securities Act 2015 which requires academy's to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of the academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes

are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The academy / academy will therefore seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites*

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff as part of safeguarding training. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by the office manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.
- The passwords for the academy ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The office manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.

- The academy has provided enhanced / differentiated user-level filtering
- Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly. The academy infrastructure and individual workstations are protected by up to date virus software.
- An agreement is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the academy systems through the academy induction process.
- An agreed policy is in that it forbids staff from downloading executable files and installing programmes on academy devices.

Mobile Technologies

Mobile technology devices may be provided might include:
smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the academy's wireless network. The device then has access to the wider internet, which may include the academy's learning platform and other cloud based services such as email and data storage.
All users should understand that the primary purpose of the use of mobile devices in an academy context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education.

Mobile Technologies with cameras

Camera mobile phones are becoming increasingly popular. A built in digital camera enables users to take high quality pictures, these can then be sent instantly to other mobile phones or email address. They can also be posted on the internet or in chat rooms. There is the potential for camera mobile phones to be misused in schools as they can become an instrument of bullying or harassment directed against pupils and staff.

The use of mobile technologies by staff and visitors:

Visitors

All visitors to school are required to not use their mobile technologies within the school unless permission has been granted. Should any visitors require access/use of their mobile phone they can request to use it in the designated area within the school entrance. All visitors to school are requested to complete the sign-in system at the office, who will provide them with a visitor lanyard during their visit to school.

Staff

Staff use of mobile phones during their working school day should be:

- Outside of their contracted hours
- Discreet and appropriate e.g. not in the presence of pupils
- Mobile phones should be switched off and stored in a safe place not accessible by staff or children especially during lesson times. School will not take responsibility for any items that are lost or stolen.
- Where a phone call is expected upon the mobile phone, this must be granted by the Headteacher or Deputy Headteacher and staff are advised to leave it with staff in the main office. They will be informed if the call is received.
- Staff are advised to give the school telephone number to be contacted upon during the school day.
- School trips/ residentials – staff are required to take a mobile phone to ensure they have full contact with school in case of an emergency. In such cases staff are expected to carry the phone upon themselves and if appropriate ensure it is not on silent.
- Staff are reminded of policy to not use for any other reason other than in communication with school or in an emergency.
- Strictly no photos should be taken of the children or activities. A school camera should be used for any photos.
- Staff should never contact pupils or parents from their personal mobile phone, or give them their mobile number to pupils or parents. If a member of staff needs to make telephone contact with a parent or pupil, a school telephone should be used.
- Staff should never send to, or accept from, colleagues or pupils, text or images that could be viewed as inappropriate. With regard to camera mobile phones, a member of staff should never use their phone to photograph a pupil(s), or allow themselves to be photographed by a pupil(s).

This guidance should be seen as a safeguard for members of staff, the school. Staff should understand that failure to comply with this policy is likely to result in the enforcement of our whistleblowing policy and associated procedures.

Pupils

While we fully acknowledge a parent's right to allow their child to bring a mobile phone to school if they walk to and from school without adult supervision (year 5 / 6), Ackton Pastures Primary Academy discourages pupils from bringing mobile phones to school due to the potential issues outlined above. When a child needs to bring a phone into school it should be left in the school office, locked until the end of the school day. Parents are advised that we accept no liability for the loss or damage to mobile phones which are brought into the school or school grounds. If a pupil is found taking photographs or video footage with a mobile phone of either other pupils or members of staff, this will be regarded as a serious offence and disciplinary action

may be taken according to the school's Behaviour Policy. If images of other pupils or members of staff have been taken, the phone will not be returned to the pupil until the images have been removed by the pupil's parent in the presence of a senior member of staff.

Many phones, especially smart phones, immediately share photos within an icloud or similar storage facility. Assurance needs to be given by a parent/carer that this is deleted. Should a pupil be found to be using a phone inappropriately, the school reserves the right to withdraw this privilege and they will no longer be able to bring a phone into school. Should parents need to contact their child or vice versa, this should be done following the usual school procedures.

Parents

While we would prefer parents not to use their mobile phones while on school premises, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times. We, therefore, ask that parents' usage of mobile phones, whilst on the school site is courteous and appropriate to the school environment.

We do allow parents to photograph or video school events such as shows or sports day using their mobile phones of their own child – but insist that parents do not publish images (eg on social networking sites) that include any children other than their own.
Parents/carers are reminded of this at the start of every school performance, on sports day, etc and will receive written reminder in the Newsletter at the start of the academic year.

The academy Acceptable Use Agreements for staff and pupils will give consideration to the use of mobile technologies

	School Devices			Personal Devices		
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Pupil/Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes	Yes	Yes
Full network access	*Yes*	*Yes*	*Yes*	No	No	No
Internet only						
No network access						

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded

themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the academy website / social media / local press
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act); parents are reminded of these procedures during concerts and other parental events. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy / academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The academy ensures that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer - N Stott (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the academy currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

When using communication technologies the academy considers the following as agreed practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the academy email service to communicate with others when in academy, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. (https://boost.swgfl.org.uk/)
- Any digital communication between staff and students or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / careers or academy staff
- They do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy, local authority or MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official academy social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving two members of staff.
- A code of behaviour for users of the accounts, including:
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under academy disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy and can be found in the academy 'social Media Policy'.
- Personal communications which do not refer to or impact upon the academy are outside the scope of this policy

- Where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the academy
- The academy should effectively respond to social media comments made by others according to a defined policy or process – Social Media policy.

The academy's use of social media for professional purposes will be checked regularly by the Online Safety Group to ensure compliance with the academy policies.

Dealing with unsuitable / inappropriate activities

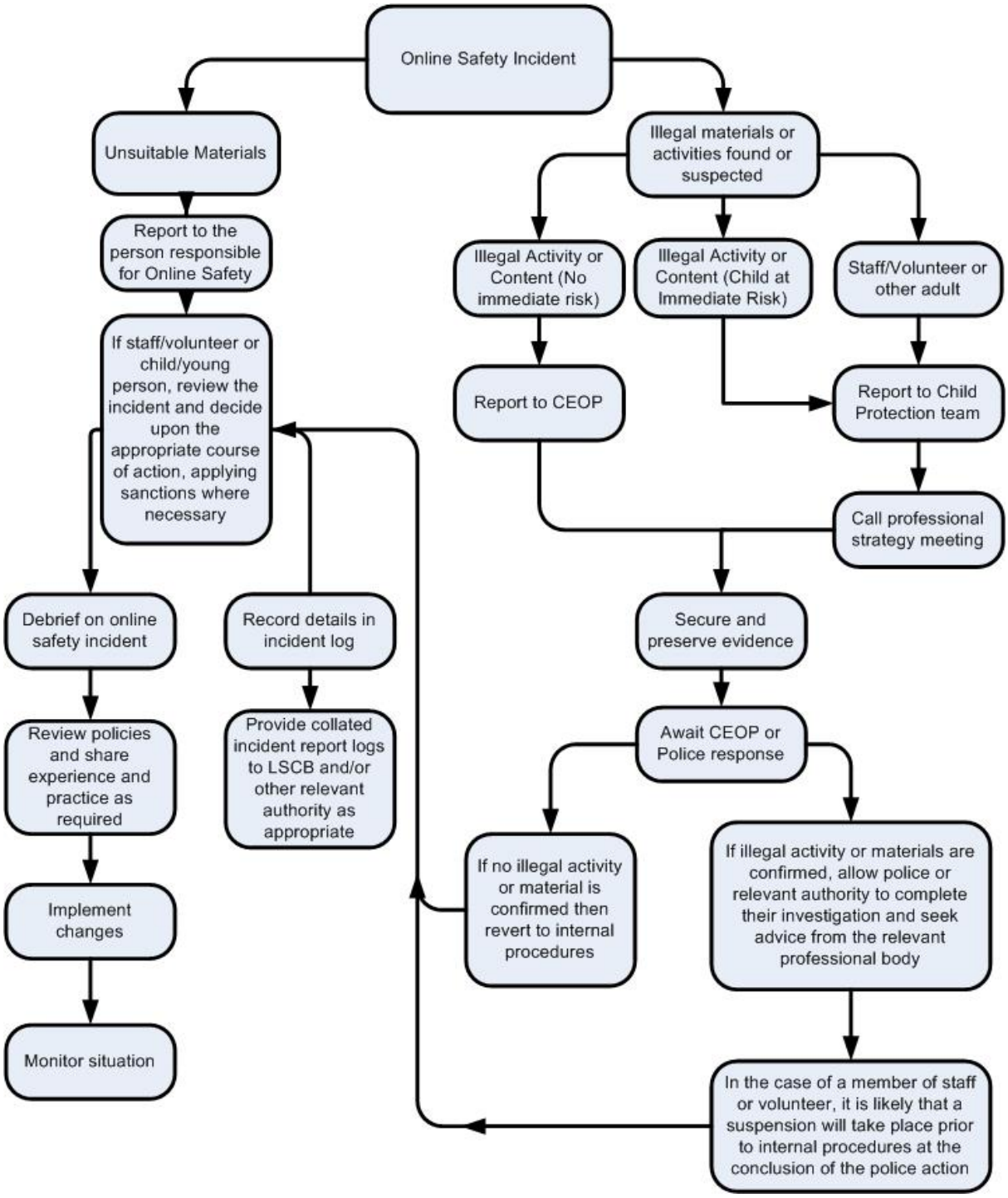
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.
The academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority, MAT (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *academy* and possibly the police and demonstrate that visits to these

sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Appendices

Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1) 26

Parent / Carer Acceptable Use Agreement Template 27

Staff (and Volunteer) Acceptable Use Policy Agreement Template 29

Responding to incidents of misuse – flow chart 35

Record of reviewing devices / internet sites (responding to incidents of misuse) 35

Pupil Acceptable Use Agreement Template – for older students / pupils

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within academys and outside academy. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *academy*:

- I will only use my own personal devices (mobile phones / USB devices etc) in academy if I have permission. I understand that, if I do use my own devices in the *academy*, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any academy device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed When using the internet for research or recreation, I recognise that:
- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of academy:

- I understand that the *academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of academy and where they involve my membership of the academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to academy systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to academy systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the academy systems and devices (both in and out of academy)
- I use my own devices in the academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy eg communicating with other members of the academy, accessing academy email, VLE, website etc.

Name of Student / Pupil: .....
Group / Class: .....
Signed: .....
Date: .....

Parent / Carer Countersignature

Signed: .....
Date: .....

Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Signed (parent): .....

Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within academys and outside academy. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the academy expectations of the young people in their care.
Parents are requested to sign the permission form below to show their support of the academy in this important aspect of the academy's work.

Permission Form

Parent / Carers Name: .....
Student / Pupil Name: .....

As the parent / carer of the above *pupil*, I give permission for my child to have access to the internet and to ICT systems at academy.

Either: (KS2 and above)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of academy.

Or: (KS1)

I understand that the academy has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of academy.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
I understand that my son's / daughter's activity on the systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the academy if I have concerns over my child's online safety.
Signed: .....

Date: .....

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of academy. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media. Where an image is publically shared by any means, only your child's initials will be used.
The academy will comply with the Data Protection Act and request parent's / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
Parents / carers are requested to sign the permission form below to allow the academy to take and use images of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent / Carers Name:..... Student / Pupil Name:.....

As the parent / carer of the above student / pupil, I agree to the academy taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
• *to support learning activities.*	Yes / No
• *in publicity that reasonably celebrates success and promotes the work of the academy.*	Yes / No
Insert statements here that explicitly detail where images are published by the academy / academy	Yes / No
I agree that if I take digital or video images at, or of – academy events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....
Date: .....

Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

Staff (and Volunteer) Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of academy, and to the transfer of personal data (digital or paper based) out of academy. I understand that the academy digital technology systems are primarily intended for educational use and that I will

only use the systems for personal or recreational use within the policies and rules set down by the academy. (academys should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of academy systems)

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in academy in accordance with the academy's policies.
- I will only communicate with students / pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy, MAT and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems.

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant academy / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy / academy policies.
- I will not disable or cause any damage to academy / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in theAcademy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *academy*:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy / academy digital technology equipment in academy, but also applies to my use of academy / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy / academy
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / MAT / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the academy digital technology systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of academy digital technologies will be responsible users and stay safe while using these systems and devices
- that academy / academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use academy systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the academy / academy:

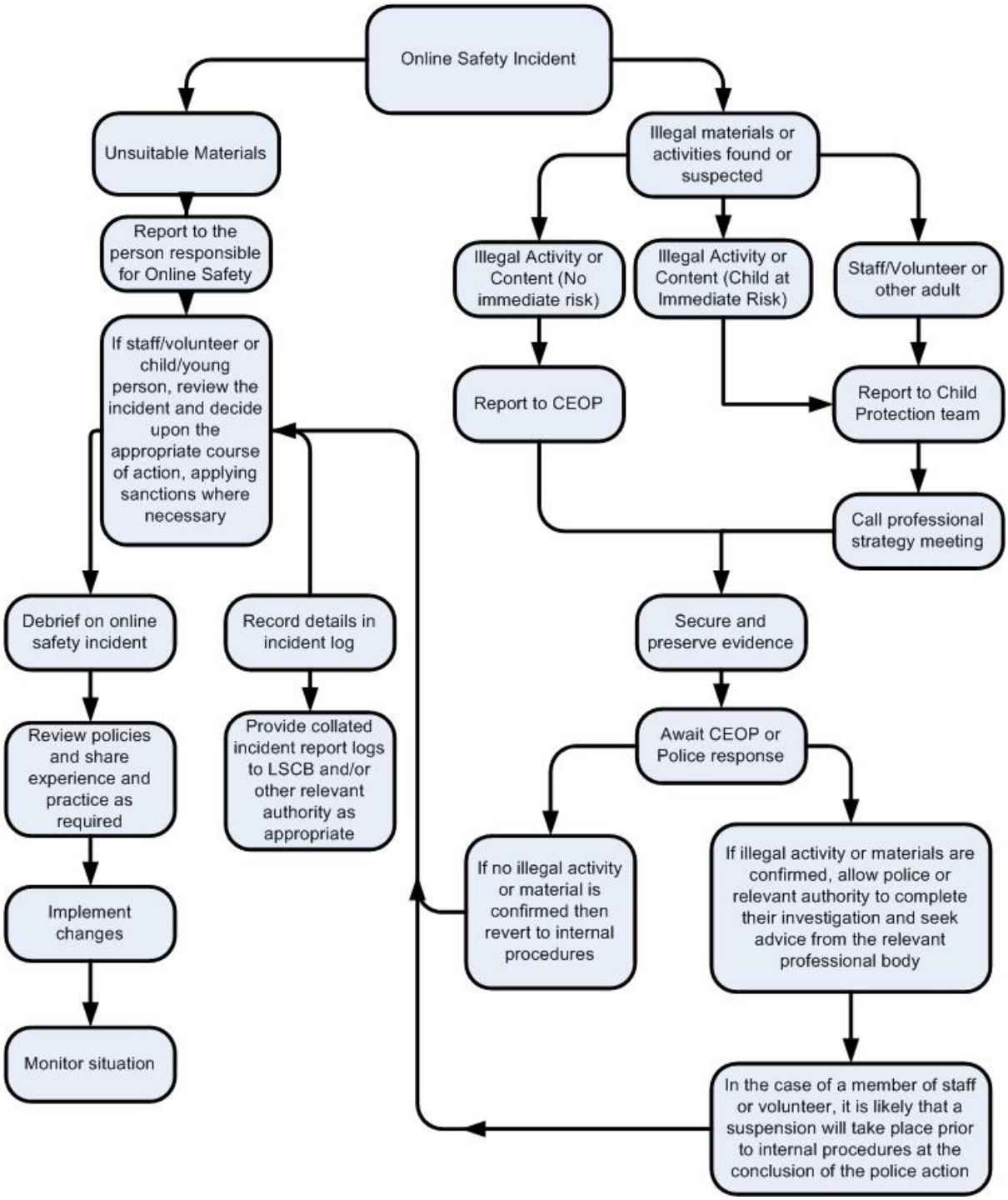
- I understand that my use of academy systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into academy for any activity that would be inappropriate in an academy setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the academy on any personal website, social networking site or through any other means, unless I have permission from the academy.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a academy device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to academy / academy equipment, or the equipment belonging to others.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the academy / academy has the right to remove my access to academy systems / devices

I have read and understand the above and agree to use the academy digital technology systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Name: .....
Signed: .....
Date: .....

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address / Reason for concern device

Conclusion and Action proposed or taken
